CollECTeR 2007, 9-11 December, Melbourne Australia

Minimising Legal Risks in Electronic Contracting[1]

Judith McNamara
Queensland University of Technology
j2.mcnamara@qut.edu.au

Kathryn O'Shea
Queensland University of Technology
k.oshea@qut.edu.au

Abstract

The use of information and communication technology (ICT) in electronic contracting has associated legal risks that must be addressed by contracting parties. The purpose of this paper is to identify the legal risks that may arise from the use of ICT in the electronic formation, administration and retention of contracts and to make recommendations to minimise these risks. The paper will conclude that collaboration platforms have the potential to minimise many of the risks associated with electronic contracting, provided they are used in conjunction with appropriate contractual provisions addressing the legal issues that arise.

1 Introduction

New ICT is increasingly playing a pivotal role in the efficient administration and management of contracts. The role of ICT in electronic contracting may vary, depending upon the sophistication of the system used and the needs of the contracting parties. Although commonly used for communication purposes, ICT may also facilitate electronic document management and collaboration between multiple parties. While ICT can result in administrative efficiencies that potentially benefit all contracting parties, a number of legal and contracting risks arise from its use for electronic contracting. Many of these risks can be addressed by adopting an appropriate electronic system, such as a collaboration platform, that incorporates various security and auditing features.

A collaboration platform is an electronic network linking organisations for the purpose of exchanging information electronically [19]. Documents are created, retained and communicated on an electronic project database. The platform is usually provided by a third party service provider who also maintains the electronic database and who has a contractual arrangement with at least one of the parties using the platform [10]. The key feature of a collaboration platform is that it enables parties to collaborate with each other regardless of whether they are located in different geographic areas and in different time zones [7]. Collaboration platforms facilitate not only communication between the parties, but also collaboration on project documents and drawings. Collaboration platforms can be used whenever electronic integration of contracting parties is required, such as for supply chain management [6].

The use of collaboration platforms has led to considerable efficiencies in the administration of contracts, particularly in the construction industry, by eliminating delays, providing

[1] This paper is based on the results of research conducted for the Australian Cooperative Research Centre for Construction Innovation Research Project 2005-025-A *Electronic Contract Administration – Legal and Security Issues*.

document control and security, improving productivity through administrative efficiencies, decreasing costs of paper document production and delivery and reducing disputes due to the audit trail of the project that is captured by the platform [17], [13]. However, the potential users of a collaboration platform must be aware of the legal risks that may arise from their use and take active steps to minimise the risks.

This paper identifies the legal risks that may arise from the use of ICT in electronic contracting. It also makes a number of recommendations to minimise these risks. The paper will conclude that collaboration platforms have the potential to minimise many of the risks associated with electronic contracting, provided they are used in conjunction with appropriate contractual provisions that address the identified legal issues. The legal risks can be broadly categorised as: risks resulting from electronic contract formation, risks in the electronic administration of contracts and risks resulting from the electronic retention of records [3].

2 Risks in electronic contract formation

Regardless of whether a contract is formed through electronic or paper based communications, the general law contractual principles that have been developed through court decisions will apply to the contract. In addition to these principles, where a contract is formed in an electronic environment the electronic transactions legislation in each jurisdiction in Australia is also relevant. The electronic transactions legislation is based upon UNCITRAL's Model Law on Electronic Commerce 1996 and on a Commonwealth level, is known as the *Electronic Transactions Act 1999* (Cth) ('ETA').[2]

In the context of electronic contract formation, a range of legal uncertainties and risks arise as a consequence of the application of traditional contract law principles to new technology, the minimalist approach adopted in the electronic transactions legislation and the interplay between the legislation and general law principles. The legal uncertainties and risks associated with electronic contract formation are briefly outlined below, together with recommendations to minimise these risks.

2.1 Time of contract formation

When parties choose to form their contract using an electronic communication method, such as a collaboration platform, difficulties may arise in determining the precise point in time that the contract has been formed. The usual position under the general law is that the acceptance of an offer (which constitutes the formation of a contract) is effective at the time it is communicated to the offeror (*Byrne & Co v Leon Van Teinhoven and Co* (1880) 5 CPD 344). When communication occurs, it is said that the parties have reached agreement or consensus upon the terms of the contract [9].

A deviation from the general position is the 'postal acceptance rule', which generally applies where the offeror and the offeree communicate by post. If the postal acceptance rule applies, the time of contract formation is brought forward such that the acceptance of an offer is effective and the contract is formed at the time the acceptance is posted, rather than when it is communicated to the offeror (*Henthorn v Fraser* [1892] 2 Ch 27).

[2] The relevant legislation in each jurisdiction of Australia is: *Electronic Transactions (Queensland)* Act *2001* (Qld); *Electronic Transactions Act 2000* (NSW); *Electronic Transactions (Victoria) Act 2000* (Vic); *Electronic Transactions Act 2000* (Tas); *Electronic Transactions (Northern Territory) Act 2000* (NT); *Electronic Transactions (Australian Capital Territory) Act 2000* (ACT); *Electronic Transactions Act 2000* (SA); and *Electronic Transactions Act 2001* (WA)).

The courts have held that the postal acceptance rule will not apply to telephone, telex and facsimile communications. However, the applicability of the postal acceptance rule to contractual communications via relatively recent technologies such as email and the world wide web has not been finally settled by the courts (although some non-definitive suggestions to the effect that the postal acceptance rule should not apply to these technologies appears in the first instance decision of the Singapore High Court in *Chwee Kin Keong v Digilandmall.com Pte Ltd* [2004] 2 SLR 594). Whilst the electronic transactions legislation in each jurisdiction in Australia contains provisions to clarify when an electronic communication is dispatched and received (eg s 14 ETA), the provisions do not resolve the issue as they fail to clarify whether it is the dispatch or the receipt of a communication that completes the formation of a contract [8], [16], [4].

Although the legal position as to the time of contract formation may be uncertain in the context of electronic communications, these uncertainties can be avoided by including provisions in a contractual offer that state how acceptance is to be communicated and when acceptance of the offer is deemed to be effective [14], [9].

2.2 Place of contract formation

The legal uncertainties surrounding the time of formation of an electronic contract make it difficult to ascertain the place where the contract has been formed. The place of contract formation is one way that a court may assume jurisdiction to hear a dispute arising out of the contract [8]. Whilst the electronic transactions legislation contains provisions relating to where an electronic communication is taken to have been dispatched and received (eg s 14 ETA), the provisions do not specify whether it is the place of dispatch or the place of receipt of a communication that is the place of contract formation [8]. However, if a contract contains clear provisions pursuant to which the parties agree to submit to the jurisdiction of the courts of a particular place and to the applicable law to govern the contract, the legal significance of the place of contract formation is minimised.

2.3 Statutory requirements for certain contracts to be in writing and signed

As a general principle, the majority of contracts will be enforceable irrespective of whether or not they are in writing or signed. However, in most jurisdictions in Australia there are legislative provisions that require particular categories of contracts to be ‘in writing’ and ‘signed’ in order to be enforceable. The main categories of contracts affected by these requirements are land contracts and guarantees (eg ss 59 and 56 *Property Law Act 1974* (Qld)). Where a land contract or contract of guarantee is formed by electronic communications, the question that arises is whether the contract is ‘in writing’ and ‘signed’?

2.3.1 Requirements of writing: The electronic transactions legislation contains provisions designed to allow requirements of writing to be satisfied in the context of electronic communications (eg s 9 ETA). There has only been one judicial decision to date that has considered this aspect of the legislation and its application to a statutory writing requirement, but the decision did not devote any time to the issue and appeared to presume that printed electronic communications (in this case emails) would amount to writing (*Faulks v Cameron* (2004) 32 Fam LR 417). There are a range of legal issues that arise from the interpretation of the ‘writing’ provisions in the electronic transactions legislation which, until resolved by the courts, make it difficult to predict whether the legislation can be relied upon to establish that an electronic guarantee or land contract is in writing. However,

notwithstanding these uncertainties, it appears that general law contractual principles have sufficiently progressed to establish that a printed electronic communication will in fact be a communication that is in writing (eg *McGuren v Simpson* [2004] NSWSC 35, which is also consistent with many decisions in the United States of America and a recent decision of the Singapore High Court).[3] The position with respect to purely electronic communications that are never reduced to physical form continues to remain unclear.

2.3.2 Signature requirements: An electronic signature may take a variety of forms, including: a type-written name, the pasting in of a scanned version of a signature, clicking an 'I Accept' button, the use of a user id and password and cryptographic technology such as digital signatures. The electronic transactions legislation contains provisions designed to allow a signature requirement to be met in the context of electronic communications (eg s 10 ETA). The only court decision relating to this aspect of the legislation held that a typed name in an email was enough to satisfy a statutory signing requirement, but the decision must be treated with caution as it did not involve a land contract or a guarantee and the court's analysis did not sufficiently address a number of issues that arise in connection with the legislation (*Faulks v Cameron* (2004) 32 Fam LR 417). The critical factors that may prevent a party from relying on a particular electronic signature method to satisfy a statutory signing requirement are that: having regard to all the relevant circumstances the signature method must be as reliable as appropriate for the purposes for which the information was communicated and the person to whom the signature is required to be given must have consented to the use of the relevant signature method.

The general law is also unclear on this issue. In Australia one court decision has applied a legal doctrine known as the 'authenticated signature fiction' to hold that a type-written name in an email was sufficient to satisfy a statutory signing requirement (*McGuren v Simpson* [2004] NSWSC 35). The difficulties associated with this case are that it did not involve a land contract or guarantee, the States and Territories have adopted different positions on the authenticated signature fiction and there has been no decision that has applied this legal doctrine to a land contract or guarantee in electronic form. Although there are authorities in the United States and Singapore to the effect that type-written names in emails are enough to satisfy signing requirements of this nature, the position within Australia is not yet sufficiently clear.[4] As a land contract or guarantee will not be enforced by the courts if it has not been

[3] In the United States of America, see *Dow Chemical Company v G.E*., 2005 US Dist. LEXIS 40866 (E.D. Mich. 2005); *Bazak International Corp v Tarrant Apparel Group*, 2005 US Dist. LEXIS 14674 (S.D.N.Y 2005); *International Casings Group Inc. v Premium Standard Farms Inc*, 2005 US Dist. LEXIS 3145 (W.D. Mo 2005); *Lamle v Mattel Inc*., 2005 US App LEXIS 217 (Fed. Cir. 2005); *Roger Edwards LLC v Fiddes & Sons*, 245 F.Supp. 2d 251 (D. Me. 2003); *Rosenfeld v Zerneck*, 4 Misc. 3d 193, 776 N.Y.S.2d 458, 2004 N.Y. Misc. LEXIS 497 (2004); *Cloud Corporation v Hasbro Inc*., 314 F. 3d 289 (7th Circ. Ill 2002); *Shattuck v Klotzbach* 14 Mass. L. Rep 260 (Mass. Super. Ct. 2001). In Singapore, refer to *SM Integrated Transware Pty Ltd v Schenker Singapore (PTE) Ltd* [2005] 2 SLR 651.

[4] In the United States of America, see *Dow Chemical Company v G.E*., 2005 US Dist. LEXIS 40866 (E.D. Mich. 2005); *Bazak International Corp v Tarrant Apparel Group*, 2005 US Dist. LEXIS 14674 (S.D.N.Y 2005); *Lamle v Mattel Inc*., 2005 US App LEXIS 217 (Fed. Cir. 2005); *Roger Edwards LLC v Fiddes & Sons*, 245 F.Supp. 2d 251 (D. Me. 2003); *Rosenfeld v Zerneck*, 4 Misc. 3d 193, 776 N.Y.S.2d 458, 2004 N.Y. Misc. LEXIS 497 (2004); *Cloud Corporation v Hasbro Inc*., 314 F. 3d 289 (7th Circ. Ill 2002); *Shattuck v Klotzbach* 14 Mass. L. Rep 260 (Mass. Super. Ct. 2001). In Singapore, refer to *SM Integrated Transware Pty Ltd v Schenker Singapore (PTE) Ltd* [2005] 2 SLR 651.

signed, for the time being all guarantees and land contracts should continue to take place in paper form using physical handwritten signatures.

3 Risks in electronic contract administration and management

The administration of contracts in an electronic environment results in a number of legal uncertainties and risks. These uncertainties and risks are briefly outlined below, together with recommendations to minimise them. It is apparent that many of these risks may be addressed by the use of a collaboration platform to administer the contract, however the use of a platform may itself lead to further legal risks which must be addressed by the parties prior to adopting the technology.

3.1 Electronic variations and notices

To a large extent, the questions of whether electronic communications can be effective to vary or amend a contract and whether notices under a contract may be given in electronic form depend upon the terms of the contract itself. The real dangers arise when the contract fails to specifically address the status of electronic communications. The legal risks include: email traffic passing between the parties may give rise to an effective variation of the contract (for example, see the English decision in *Hall v Cognos Ltd* (Industrial Tribunal Case No. 1803325/97)); even if the parties intend to be bound by electronic variations, the legal position will depend upon the terms of the contract and the parties' conduct; and disputes will invariably arise in relation to the validity of electronic contractual notices. Neither the general law nor the electronic transactions legislation provide simple answers to these legal risks.

The most effective way to combat the risks described above is to incorporate appropriate provisions within a contract that address the following matters:

- The parties' intentions as to the status of electronic communications must be made clear in the contract. If the parties do not wish to be bound by electronic communications and notices then this should be stated in the contract.
- If the parties do wish to be bound by electronic communications they should decide whether they wish to use electronic communications for all or only some contractual communications and notices. The contract must be clear as to which communications may and may not be delivered electronically [2].
- The electronic communication method to be used by the parties should be identified, together with the relevant electronic addresses and details of authorised recipients.
- If the parties intend to utilise electronic communications, then they should expressly consent to the use of electronic communications, but only to the extent specified in the contract.
- The contract must include a timing provision governing when electronic communications are deemed to have been received (which will in large part, depend on the communication system being used and the acceptability of the timing provision to both contract parties).
- Contracts commonly require notices and communications to be writing and signed. The contract should deem notices and communications that may be delivered in electronic form to be in writing and signed. For signature requirements, the

contract should identify the electronic signature method that will be used by the parties, the parties should consent to the use of that method and acknowledge that it is considered by them to be both reliable and appropriate.

- It is possible that the specified electronic communication method to be used by the parties may become unavailable from time to time. The contract should contain alternative communication protocols for the parties to follow in the event that this occurs.

3.2 Disruptions caused by unavailability of technology

The unavailability of the electronic system used to administer a contract may result in delays and increased costs for the contracting parties. This may be of particular concern where a collaboration platform is the primary ICT used to administer the contract because its unavailability will simultaneously impact upon all parties to the contract. The platform could become unavailable for a range of reasons – for example, as a consequence of technical difficulties, or because the service provider is no longer in business.

To minimise the risk of costs being incurred due to the unavailability of a collaboration platform being used to administer a contract, the contract with the service provider should include provisions relating to disruptions to the platform [19]. The types of provisions that should be considered include: details of any scheduled service disruptions, the notifications that must be given in the event of any unscheduled downtime, what will happen in the event of the platform crashing unexpectedly and the arrangements to take place in the event that the service provider becomes insolvent.

While the contract with the service provider can provide for contingencies in the event of the platform being unavailable, it cannot eliminate the risk of disruption as a result of such unavailability. Accordingly, users of a collaboration platform should consider taking out business interruption insurance that covers them in the event the platform becomes unavailable [1].

3.3 Contractual arrangements with the service provider of a collaboration platform

There may be disputes that arise between the service provider of the collaboration platform used to administer a contract and the contracting parties who are the users of the platform. For example, the capacity of the platform in terms of the number of users who can simultaneously access the platform may not be as represented by the service provider or as expected by the users of the platform. To minimise disputes between the service provider and the users of the platform, the contract with the service provider should include specific provisions that clarify the rights and obligations of the service provider. The following types of provisions should be included in the relevant contract [19]:

- Technical specifications as to the levels of service to be provided including specifications as to security, backup systems, integrity of data, audit trails, access controls, system availability, software upgrades, customer support and end-user training;
- A licence to the contracting parties to use the platform for the purposes of the project;
- The use which may be made of the project data by the service provider and the project participants;

- Express identification of the ownership of the copyright in the collaboration platform;
- Any right of the service provider to use the project participants' branding and data;
- Indemnification of the service provider against the unauthorised use of the collaboration platform;
- A specific duty of confidentiality which should include the security of user names and passwords;
- Any limitations upon the liability of the service provider; and
- The allocation of responsibility for the archiving and storage of the project database upon completion of the project.

Sometimes only one of the contracting parties will be in a contractual relationship with the service provider of the platform. In that case, the service provider should also enter end user licence agreements with any contracting parties who are not the customers of the service provider. Ideally these agreements should be identical to each other and should be annexed to the contract between the contracting parties[19].

3.4 Potential disputes between the contracting parties

In addition to the possibility of the contracting parties becoming involved in a dispute with the third party service provider, there is a risk that the electronic administration of a contract may lead to disputes between the parties. There is also a risk that if the contracting parties become involved in a dispute that leads to litigation, the fact that the project has been administered electronically may complicate the litigation. To minimise such disputes, the contract should contain specific provisions relating to the electronic administration of the project. The issues that may arise in relation to disputes between the contracting parties relate to:

- ownership of intellectual property;
- breaches of confidentiality of project records;
- the use of electronic records as evidence in the event of litigation of a dispute; and
- compliance with the parties' obligations to make disclosure to each other of relevant documents in the event of a dispute resulting in litigation.

3.4.1 Intellectual property: Where a contract involves plans, drawings or other documents to which copyright attaches that are submitted electronically, there may be a concern that the copyright in the drawings could be infringed more easily due to the ease with which copies of the drawings can be made and distributed. To minimise the risk of copyright infringements, designers should take practical steps to protect their copyright in the drawings, including incorporation by watermark of a copyright statement and disclaimer [19].

The general legal position is that the original designer is the owner of the copyright in plans and drawings (s 35 *Copyright Act 1968* (Cth)). There may be contractual provisions that grant an assignment of the copyright or a licence to use the plans in relation to the particular project. For example, in relation to a construction project, the contract between the principal contractor and the designer may contain an assignment of the copyright in the drawings to the principal contractor or the owner of the building, or the grant of a licence to the principal

contractor and other contractors to use the design in relation to the project [19]. Even if the contract does not contain such an assignment or licence, there would be an implied licence to use the drawings for the purposes of the project (*Gruzman Pty Ltd v Percy Marks Pty Ltd* (1989) 16 IPR 87; *Concrete Pty Ltd v Parramatta Design & Developments Pty Ltd* (2006) 231 ALR 663). The legal position in relation to the ownership of copyright in the project drawings would not normally change as a result of the electronic administration of the contract.

However, if a drawing or other document is amended extensively by collaboration, there is a risk that the collaborators will be seen to be the joint authors of the drawing. In that case the ownership of the copyright in the drawing may no longer rest with the original designer but with the collaborators jointly [19]. To avoid doubt arising as to the ownership of copyright, the contract should specifically provide for the ownership of copyright in the drawings and other documents and such provision should be specified to continue to apply regardless of the extent of collaboration between the parties in their development.

3.4.2 Confidentiality: The confidentiality of electronic records may be compromised either as a result of one of the contracting parties disclosing the records to an unauthorised person or by a person obtaining unauthorised access to the electronic database. To ensure that there is a legal remedy in the event of an unauthorised disclosure by one of the contracting parties, the contract between the contracting parties should include a specific duty of confidentiality. In addition, the parties should ensure that the technology used to administer the contract employs appropriate access controls and authentication mechanisms to ensure that only authorised persons can access the records. These security features are generally present in collaboration platforms. Ordinarily, collaboration platforms implement access controls which ensure that only authorised persons have access to records, in particular a role based access control policy will ensure that access rights are assigned to individuals depending on their role within an organisation. In addition, collaboration platforms employ authentication mechanisms such as user names and passwords, and internet protocol authentication.

3.4.3 Evidentiary issues: In the event that there is a dispute between the parties, there may be some doubt as to the reliability of electronic records as evidence in court. The key issues are whether or not electronic records are admissible and if they are, what weight will be given to them by a court.

A court may find that electronic records are inadmissible as evidence if they are considered to be hearsay (i.e. they contain a statement by a human and are relied upon as evidence of the truth of such statement: *Walton v The Queen* (1989) 166 CLR 283, 288). However, it is likely that electronic records created and maintained by a collaboration platform will be admissible under the business records exception to the hearsay rule (eg s 69 *Evidence Act 1995* (Cth)). To minimise any risk that electronic records would not be admissible, the agreement between the contracting parties should include a provision deeming electronic records maintained by the agreed system to be admissible as evidence and prima facie accurate [15].

Even if an electronic record is admissible as evidence it is for the court to determine how much weight to give to the record. The court may give less weight to the evidence or even find it to be inadmissible if it is unreliable. An electronic record may be considered by a court to be unreliable as evidence if the parties cannot prove that the electronic record presented to the court is the original record or an accurate copy of it. The integrity of an electronic record

may be questioned if the party relying on it cannot prove that it has not been altered by human intervention or corrupted by computer malfunction [11]. The security and management of the relevant electronic storage system will impact upon whether a court is likely to consider electronic records as reliable evidence [5]. If a collaboration platform is used to create and maintain a record, the platform's logging and auditing trails, authentication mechanisms and access controls will help to establish the integrity of the electronic record.

3.4.4 Discovery: In the event that a dispute results in litigation the parties may be required to make disclosure to each other of records that are relevant to the dispute. This disclosure process may be costly and time consuming if there is a multitude of electronic copies of records held on a range of electronic devices [18]. A collaboration platform will assist the parties to identify and locate all relevant copies of electronic records in order to satisfy their disclosure obligations in a timely and cost effective manner. Where a collaboration platform is used, the parties should not use any other electronic systems for the creation or communication of electronic records as this will complicate the disclosure process.

4 Risks in electronic record keeping and archiving

Various Commonwealth and State legislation impose obligations on individuals and organisations to maintain records. For example, the *Income Tax Assessment Act 1997* (Cth) requires tax records to be kept for five years and the *Corporations Act 2001* (Cth) requires companies to keep written financial records for seven years. The electronic transactions legislation allow for such records to be kept electronically provided that the information in them remains accessible and the method used for storing them is reliable for maintaining their integrity (eg s 12 ETA). If electronic records are not archived in a manner that ensures that they remain accessible and that maintains the integrity of the records, the parties may be in breach of these statutory obligations. The accessibility or integrity of electronic records may not be able to be assured if the storage media on which they are kept breaks down over time [12], or if technology changes mean that it is no longer possible to access the records [5].

Parties who administer a contract electronically should ensure that they implement a record keeping system that assures the accessibility and integrity of the electronic records. Collaboration platforms record all iterations of records created using the platform and use auditing and logging features which will enable parties to demonstrate at a later time that a record has not been altered since its creation. However, parties should ensure that upon completion of the project, the service provider of the platform continues to maintain the platform software to ensure that records are able to be accessed in the future. The agreement with the provider of the collaboration platform should contain provisions for the archiving of project records and should specify the technical standards to be met in archiving the data. The contractual provisions should also specify who is to bear the cost of archiving the data and, if the data is required to be accessed, the access procedure and the party who is to bear the access costs [1].

A further risk in relation to the archiving of electronic records is that where a third party service provider is responsible for the archiving of the records, the parties may not be able to obtain access to them if the third party is no longer in business. To address this possibility it is recommended that a copy of the project data should be provided to each of the contracting parties on a CD R/W disk [19].

In addition, where one of the contracting parties is a government agency, the agency must comply with its statutory obligation to retain public records. Government agencies' record keeping obligations vary between State and Commonwealth jurisdictions,[5] however generally, if a third party service provider is responsible for the maintenance of the electronic database, the agency must make arrangements for the safe keeping, proper preservation and return of the records. It may not be clear what steps a government agency must take in order to comply with the relevant government recordkeeping framework when a collaboration platform is used. It is recommended that before agreeing to the use of a collaboration platform, a government agency should ensure that the platform will comply with the agency's record keeping obligations and, if there is any doubt in this regard, clarification should be sought from the relevant State Archivist.

5 Conclusion

Our research has identified many risks associated with electronic contracting which may lead to serious practical consequences for contracting parties. On a more general level, these risks may contribute to a reduced willingness by business to take advantage of modern communication technologies.

Many of the legal risks associated with electronic contracting can be minimised by appropriate contractual provisions. In addition, many of the risks associated with electronic contract administration and record keeping can also be minimised by the use of a collaboration platform which has appropriate security, authentication and auditing features. . However, the use of a collaboration platform may itself give rise to additional concerns such as: appropriate contractual arrangements between the parties (including any third party service provider), the ownership of intellectual property, the security of the platform and compliance with statutory record keeping obligations. Each of these risks must be considered and addressed by the parties prior to adopting a collaboration platform for electronic contracting purposes.

[5] The relevant legislation in each jurisdiction is as follows: *Archives Act 1983* (Cth); *State Records Act 1998* (NSW); *Information Act 2002* (NT); *Public Records Act 1996* (Qld); *State Records Act 1929* (SA); *Archives Act 1983* (Tas); *Public Records Act 1973* (Vic), and *State Records Act 2000* (WA).

REFERENCES

1 P.W. Berning, and S. Diveley-Coyne, 2000, "E-Commerce and the Construction Industry: The Revolution Is Here", October 2, 2000, available at http://www.constructionweblinks.com/Resources/Industry_Reports__Newsletters/Oct_2_2000/e-commerce.htm (accessed 15 December 2005).

2 I. Briggs, and S. Brumpton, 2001, "Embrace E-Construction With Care!", *Australian Construction Law Bulletin*, vol.13, no.4, p. 25.

3 S. Christensen, J. McNamara and K. O'Shea, 2007, "Legal and Contract Issues in Electronic Project Administration in the Construction Industry", *Structural Survey*, vol. 25, no.3-4, pp.191-203.

4 A. De Zilva, 2003, "Electronic Transactions Legislation: An Australian Perspective", *The International Lawyer*, vol.37, no.4, p.1009-1022.

5 Department of Public Works and Services New South Wales, 2000, *Risk Management in Electronic Procurement*, available at http://www.cpsc.nsw.gov.au/e-procurement/docs/Risk-Chapter2.pdf (accessed 7 December 2005).

6 M. Gogolin, 2003, "Success and Failure of Collaboration Platforms", in: Lechner, Ulrike (Hrsg.), Proceedings of the Tenth Research Symposium on Emerging Electronic Markets 2003, S. 169183, Bremen: University of Bremen, Germany, 2003 available at http://www.hsw-basel.ch/iwi/publications.nsf/b82fc4ba9fa7cb91c1257226004f8ed0/464e47ef485cf8b6c125722e002922a7?OpenDocument (accessed 7 September 2007).

7 T.M. Hassan, M.A. Shelbourn, and C.D. Carter, 2004, "Legal and Contractual Framework for the Virtual Organisation" in "Virtual Organisations, Systems and Practices", *Springer Science*, available at http://e-pub.uni-weimar.de/volltexte/2004/206/pdf/icccbe-x_257.pdf (accessed 8 December 2006).

8 S.W.B. Hill, 2001, "Email Contracts – When is the Contract Formed?", *Journal of Law and Information Science*, vol.12, no.1, pp. 46-56.

9 S.W.B. Hill, 2002, "Formation of Contracts Via Email – When and Where?", *Commercial Law Quarterly*, vol.16, no.1, pp. 3-11.

10 J. Kamara, and D.Y.H. Pan, 2004, "Virtual Collaborative Design", *Construction Information Quarterly*, vol 6, no 2, p. 56-61.

11 E. T. Laryea, 1999, "The Evidential Status of Electronic Data", *National Law Review*, Issue 3, p. 6.

12 National Office for the Information Economy, 2002, *National Electronic Authentication Council Report on Liability and Other Legal Issues in the Use of PKI Digital Certificates*.

13 P. Nitithamyong, and M.J. Skibniewski, 2006, "Success/Failure Factors and Performance Measures of Web-Based Construction Project Management Systems: Professionals' Viewpoint", *Journal of Construction Engineering and Management*, vol. 132, no 1, pp. 80-87.

14 K. O'Shea and K. Skeahan, 1997, "Acceptance of Offers by E-Mail – How Far Should the Postal Acceptance Rule Extend?", *Queensland University of Technology Law Journal*, vol.13, pp. 247-262.

15 C. Reed, 2001, "Legally Binding Electronic Documents: Digital Signatures and Authentication", *The International Lawyer*, vol.35, no.1, pp. 89-106.

16 J. Thompson, 2003, "Has the New State Electronic Transactions Act Solved All Our Problems?", *Brief*, vol.20, no.11, pp.26-27.

17 S.E. Tuma, and C.R. Ward, 2000, "Contracting Over the Internet in Texas", *Baylor Law Review*, vol.52, no.2, pp. 381-390.

18 S. White, 2001, "Discovery of Electronic Documents", *Computers & Law*, vol.44, p. 46.

19 P.Wilkinson, 2005, *Construction Collaboration Technologies: The Extranet Revolution*, Taylor & Francis, London; New York.